Felton B.V.

Verklaring van Controles bij een serviceorganisatie die relevant zijn voor Beveiliging, Beschikbaarheid en Vertrouwelijkheid (SOC 2) – Type III Rapport

Voor de periode 1 januari 2023 tot en met 31 maart 2023

Opgesteld op 30 mei 2023

Inhoudsopgave

1. SECTIE 1: MANAGEMENTVERKLARING

Wij hebben de bijgevoegde beschrijving opgesteld van het systeem van Felton B.V. met betrekking tot de Managed Services zoals geleverd door Felton B.V. (Service Organisatie) voor de periode 1 januari 2023 tot en met 31 maart 2023 (Beschrijving) in overeenstemming met de criteria voor een beschrijving van het systeem van een dienstverlenende organisatie zoals uiteengezet in de Beschrijving Criteria DC sectie 200 2018 Beschrijving Criteria voor een Beschrijving van het Systeem van een Serviceorganisatie in een SOC 2-rapport (beschrijvingscriteria).

De Beschrijving is bedoeld om gebruikers te voorzien van informatie over de Managed Services (Systeem), die nuttig kan zijn bij het beoordelen van de risico's die samenhangen met het Systeem gedurende de periode van 1 januari 2023 tot 31 maart 2023, met name informatie over beheersingsmaatregelen die de Serviceorganisatie heeft ontworpen en geïmplementeerd om redelijke zekerheid te bieden dat haar serviceverplichtingen en systeemvereisten zijn bereikt op basis van de criteria voor Beveiliging, beschikbaarheid en Vertrouwelijkheid zoals uiteengezet in TSP sectie 100, 2017 Trust Services Criteria voor Beveiliging, Beschikbaarheid, Integriteit van Processen, Vertrouwelijkheid en/of Privacy (van toepassing zijnde trust services criteria).

Felton B.V. maakt voor verschillende activiteiten gebruik van sub-serviceorganisaties zoals – maar niet uitgesloten – Cloud- en datacenterproviders, telco-providers en andere externe dienstverleners ("Sub serviceorganisaties"). De beschrijving van het systeem omvat alleen de beheersmaatregelen en relevante Trust Services Princples van Felton B.V. en sluit de Beheersdoelstellingen en gerelateerde beheersmaatregelen controles van dergelijke sub-serviceorganisaties uit. De interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld kunnen alleen worden bereikt, indien de aanvullende interne beheersingsmaatregelen van een gebruikende entiteit samen met de interne beheersingsmaatregelen van de serviceorganisatie op afdoende wijze zijn opgezet of werken.

Wij bevestigen naar eer en geweten dat:

De beschrijving een getrouw beeld geeft van het systeem van Managed Services gedurende de periode van 1 januari 2023 tot 31 maart 2023, gebaseerd op de volgende normen voor de beschrijving:

i. De beschrijving bevat de volgende informatie:
   a. De types dienstverlening.
   b. De componenten van het systeem die worden gebruikt voor de diensten:
      i. Infrastructuur. De fysieke structuren van IT en andere hardware (zoals computers, apparatuur, mobiele telefoons, communicatie netwerken).
      ii. Software. De toepassingen en systeemsoftware die deze toepassingen ondersteunt (zoals besturingssystemen, middleware, utilities).
      iii. Mensen. De medewerkers die betrokken zijn bij de governance, het gebruik en het beheer van systemen (ontwikkelaars, operators, gebruikers en managers).
      iv. Procedures. De handmatige en geautomatiseerde procedures in en rondom het systeem.
      v. Data. De informatie die door het systeem wordt gebruikt en ondersteund (bestanden, databases, tabellen, transacties).
   c. De grenzen die in de beschrijving aan het systeem worden gesteld en de aspecten die aan de orde komen.

d. Voor het verschaffen of ontvangen van informatie aan of van sub-serviceorganisaties en andere partijen,
    i. hoe dit gebeurt, wat de rol van de sub-serviceorganisatie of andere partij is
    ii. welke procedures er zijn om vast te stellen dat die informatie en werking, onderhoud en opslag daarvan onderworpen zijn aan adequate beheersingsmaatregelen.
e. De van toepassing zijnde trust services criteria en de daarmee samenhangende beheersingsmaatregelen om te voldoen aan de criteria, waaronder:
    i. Aanvullende beheersingsmaatregelen bij de gebruikende entiteit die dienen te worden overwogen in de opzet van het systeem.
    ii. In geval van toepassing van de opname methode: de beheersingsmaatregelen bij de sub-service organisatie.
f. Als gebruik wordt gemaakt van de uitsluitingsmethode voor de sub-serviceorganisatie,
    i. De aard van de diensten die worden verleend door de sub-serviceorganisatie;
    ii. De van toepassing zijnde trust services criteria die moeten worden afgedekt door beheersingsmaatregelen bij de sub-serviceorganisatie, zelfstandig of in combinatie met beheersingsmaatregelen bij de service organisatie, en de typen beheersingsmaatregelen die naar verwachting nodig zijn bij de sub-serviceorganisatie om te voldoen aan deze criteria.
g. Alle van toepassing zijnde trust services criteria die niet worden afgedekt door een beheersingsmaatregel en de reden daarvan.
h. In de situatie van een type II rapport de relevante veranderingen in het systeem van organisaties gedurende de betreffende periode.

ii. De beschrijving laat geen relevante zaken weg of geeft geen verkeerde voorstelling van zaken over het systeem en is opgesteld voor de gebruikelijke informatiebehoefte van een brede groep van gebruikers. De beschrijving dekt daarom niet alle aspecten af die een individuele gebruiker belangrijk acht.
a. De beheersingsmaatregelen die in de beschrijving zijn opgenomen zijn toereikend in opzet en bestaan gedurende de periode van 1 januari 2023 tot 31 maart 2023 om te voldoen aan de van toepassing zijnde trust services criteria.
b. De beheersingsmaatregelen die in de beschrijving zijn opgenomen zijn toereikend in opzet en bestaan en werking gedurende de periode van 1 januari 2023 tot 31 maart 2023 om te voldoen aan de van toepassing zijnde trust services criteria.

9 juni 2023,
Felton B.V.

Marnix-Jan van der Moolen

2. Sectie 2: Onafhankelijk Assurance rapport

Aan het management van Felton B.V.
Databankweg 26c
3821 AL Amersfoort

2.1 Conclusie

Wij hebben onze conclusie gevormd op basis van de zaken die in dit rapport uiteen zijn gezet. Ons oordeel, gebaseerd op de criteria uiteengezet in de vermelding van Felton B.V. en de van toepassing zijnde trust services criteria luidt dat:

a. De beschrijving een getrouw beeld geeft van ontwerp en implementatie van de dienst Managed Services gedurende de periode van 1 januari 2023, tot 31 maart 2023.

b. De beheersingsmaatregelen zoals opgenomen in de beschrijving zijn geschikt om met een redelijke mate van zekerheid te voldoen aan de van toepassing zijnde trust services criteria als deze maatregelen effectief hebben gewerkt gedurende de periode van 1 januari 2023, tot 31 maart 2023, en als de gebruikende entiteit de aanvullende beheersingsmaatregelen heeft getroffen zoals verondersteld in het ontwerp van het systeem van Felton B.V. gedurende de periode 1 januari, tot 31 maart.

c. De geteste beheersingsmaatregelen, die samen met de aanvullende beheersingsmaatregelen bij de gebruikende entiteiten, zoals beschreven in de scope-paragraaf van dit rapport, indien deze effectief werken, waren de maatregelen die nodig zijn om een redelijke mate van zekerheid te verschaffen dat de van toepassing zijnde trust services criteria worden behaald. Deze maatregelen werkten effectief gedurende de periode 1 januari 2023, tot 31 maart. De specifieke testwerkzaamheden op beheersingsmaatregelen en de aard, timing en resultaten daarvan zijn opgenomen in de sectie van dit rapport met de naam "Beschrijving van de criteria, controletest en resultaten van tests ."

2.2 Uitvoering assurance-opdracht conform 3000A & Regelement Gedragscode

Wij hebben onze assurance-opdracht uitgevoerd conform Nederlandse wetgeving en de NOREA Richtlijn Assurance-opdrachten door IT-Auditors (3000A). Deze richtlijn vereist dat wij de planning en uitvoering van onze opdracht zo inrichten dat er sprake is van een redelijke mate van zekerheid in ons oordeel.

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

2.3 Aanduiding van niveau van zekerheid & van toepassing zijnde criteria

We hebben de opdracht gekregen assurance te geven met een redelijke mate van zekerheid over de bijgaande beschrijving getiteld "Organisatieoverzicht en systeembeschrijving " over de periode 1 januari 2023 tot 31 maart 2023 (de beschrijving) gebaseerd op de criteria voor een beschrijving zoals weergegeven in DC sectie 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria), (description criteria) en de geschiktheid van de opzet en effectieve werking van beheersingsmaatregelen om te voldoen aan de criteria {Beveiliging, Beschikbaarheid, Vertrouwelijkheid} beginselen zoals uiteengezet in TSP sectie 100,

"2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy", uitgegeven door het Assurance Services Executive Committee van de AICPA (van toepassing zijnde trust services criteria) gedurende de periode van 1 januari 2023, tot 31 maart 2023.

De van toepassing zijnde criteria worden aangeduid in de vermelding van Felton B.V Service Organisatie's in combinatie met de van toepassing zijnde trust services criteria.

2.4 Beschrijving voor algemene behoefte van brede groep gebruikers

De beschrijving van de Felton B.V. Managed Services is opgesteld voor de algemene informatiebehoefte van een brede groep gebruikers en hun auditors. De beschrijving dekt daarom niet alle aspecten af die een individuele gebruiker belangrijk acht. Verder is het mogelijk dat beheersingsmaatregelen, vanwege hun aard en inherente beperkingen, niet altijd effectief werkten om te voldoen aan de van toepassing zijnde trust services criteria. Bovendien is de projectie van een eventuele beoordeling van de getrouwheid van de presentatie van de beschrijving of de conclusies omtrent de geschiktheid van de opzet of de effectieve werking naar toekomstige periodes onderhevig aan het risico dat het systeem wordt gewijzigd of dat interne beheersingsmaatregelen bij een serviceorganisatie inadequaat worden of tekortschieten.

2.5 Beoogde doelgroep van deze rapportage

Dit rapport en de beschrijving van de testwerkzaamheden en de resultaten daarvan is alleen gericht op gebruik door organisaties die gebruik maken van Felton B.V. Managed Services gedurende de gehele of gedeeltelijke periode van 1 januari 2023, tot 31 maart 2023 en onafhankelijke auditors die diensten verlenen aan deze organisaties en die voldoende kennis en begrip hebben van:

- De aard van de door de serviceorganisatie verleende diensten.
- Hoe het systeem van de serviceorganisatie samenhangt met de gebruikende entiteiten, sub-serviceorganisaties en andere partijen.
- Interne beheersing en de beperkingen daarvan.
- Aanvullende beheersingsmaatregelen bij de gebruikende entiteit en hoe deze samenhangen met de beheersingsmaatregelen bij de serviceorganisatie om de van toepassing zijnde criteria in te vullen.
- De van toepassing zijnde criteria (Trust Services Criteria).
- De risico's die van invloed zijn op het voldoen aan deze criteria en hoe beheersingsmaatregelen deze risico's adresseren.

Dit rapport is niet bedoeld voor gebruik door andere dan de hiervoor genoemde partijen en dergelijk gebruik is niet toegestaan.

2.6 Verantwoordelijkheden Serviceorganisatie

Felton B.V. heeft de bijgevoegde beschrijving van het systeem en management verklaring verstrekt, gebaseerd op de daarin geïdentificeerde criteria. Felton B.V. is verantwoordelijk voor;
(1) het opstellen van de beschrijving en de vermelding;
(2) de volledigheid, accuratesse en de presentatie van zowel de beschrijving als de vermelding;
(3) het verlenen van de diensten zoals in de beschrijving weergegeven;
(4) het specificeren van de beheersingsmaatregelen die voldoen aan de van toepassing zijnde trust services criteria en de opname daarvan in de beschrijving; en
(5) het opzetten, implementeren en documenteren van de beheersingsmaatregelen om te voldoen aan de van toepassing zijnde trust services criteria.

2.7 Verantwoordelijkheden van de auditor

Onze verantwoordelijkheid is het uitspreken van een oordeel over de getrouwheid van de presentatie van de beschrijving, gebaseerd op de criteria zoals uiteengezet in de vermelding van Felton B.V. en over hoe de opzet en werking van de beheersingsmaatregelen leiden tot het voldoen aan de van toepassing zijnde trust services criteria op basis van procedures die wij hebben gevolgd om een redelijke mate van zekerheid te verschaffen. De auditeenheid past het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhoudt het een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en procedures voor de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving.

Onze assurance-opdracht omvat het uitvoeren van procedures die assurance-informatie over de vraag of de presentatie van de beschrijving getrouw is en dat opzet en werking van de beheersingsmaatregelen voldoen aan de van toepassing zijnde trust services criteria. Deze procedures hangen af van beoordelingen door de auditor en de inschatting van het risico dat de beschrijving niet getrouw is en dat de opzet en werking van de beheersingsmaatregelen niet voldoen aan de van toepassing zijnde trust services criteria. De procedures omvatten ook het testen van de effectieve werking van die beheersingsmaatregelen die we noodzakelijk achten om te komen tot een redelijke mate van zekerheid dat wordt voldaan aan de van toepassing zijnde criteria. Onze procedures omvatten ook de beoordeling van de overall-presentatie van de beschrijving. Naar onze mening hebben we voldoende assurance-informatie verkregen om te komen tot een oordeel met een redelijke mate van zekerheid.

9 juni 2023
NewDay IT Risk &Assurance Services BV,
Bruistensingel 210
5232 AD 's-Hertogenbosch

drs A.E. Klaassen RE CIPP/E CIPM
Managing Partner

3. Sectie 3: Organisatieoverzicht en systeembeschrijving

3.1 Service commitments

Felton B.V. is opgericht in 2003 en is een Managed Service Provider voor serverbeheer, cloudbeheer, netwerkbeheer, securitybeheer, werkplekbeheer en ICT-servicedesk. Daarnaast biedt Felton met de Felton Cloud een betrouwbare en veilige Private Cloud aan haar klanten. Felton is een betrouwbare partner voor ICT-outsourcing en clouddiensten.

Felton zet zich in om doelstellingen te bereiken die voornamelijk betrekking hebben op het volgende:

- Felton opereert volgens de toepasselijke wet- en regelgeving

- Felton levert haar dienstverlening zoals beschreven in de SLA's en contracten aan haar klanten

- Felton beveiligt haar dienstverlening volgens best practices

- Felton zet zich in om zich continu op alle vlakken te verbeteren

3.1.1 Trust Services-criteria die in scope zijn op het systeem in kwestie

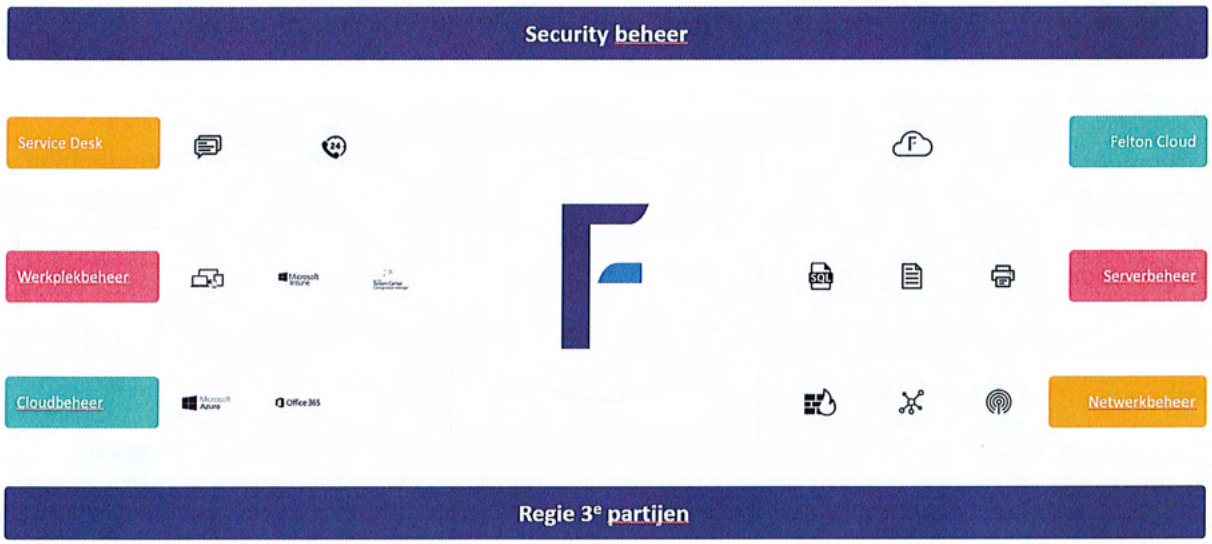
Alle criteria inzake veiligheid, beschikbaarheid en vertrouwelijkheid zijn van toepassing op het systeem van colocatie, managed hosting en managed services. De proces integriteit- en privacy criteria en de bijbehorende controles zijn niet van toepassing op het systeem.

3.2 Beschrijving van de geleverde diensten

Felton is als managed services provider gespecialiseerd in het compleet beheren van ICT-infrastructuren. Of het nu gaat om security, modern workplace, netwerken, servers, private cloud, public cloud, Office365 en/of integratie- en migratieprojecten.

Felton stelt zich op als kennispartner in ICT. Onze dienstverlening onderscheidt zich door kwaliteit, toegevoegde waarde, partnerschap en persoonlijke betrokkenheid.

Felton is verantwoordelijk voor het beheer van de omgeving, waarbij de onderliggende diensten worden geleverd op basis van de service-voorwaarden.



3.3 Componenten van het systeem

3.3.1 Infrastructuur en Software

De volgende softwaretoepassingen worden beschouwd als primaire ondersteuningssystemen die worden gebruikt ter ondersteuning van het colocatie-, managed hosting- en managed services-systeem.

Primaire Infrastructuur			
Productie Applicatie	**Beschrijving van de bedrijfsfunctie**	**Operating System Platform**	**Fysieke Locatie**
Topdesk	1. Ticketingsysteem voor changes, en incidenten. 2. CMDB	n.v.t.	Topdesk SaaS
Exact Online	1. Financiële administratie en urenregistratie 2. Personeelsadministratie	n.v.t.	Exact SaaS
Microsoft Teams & office 365	1. Samenwerkingsomgeving. 2. Centrale omgeving voor documentatie van klantenteams, sales, servicedesk, security, privacy & Quality Forum. 3. Telefooncentrale 4. videoconferencing	n.v.t.	Microsoft SaaS
Passwordstate & Roboform	Wachtwoordenkluis	Windows Server & SaaS	Felton Cloud

De volgende softwaretoepassingen worden beschouwd als secundaire ondersteuningssystemen die worden gebruikt ter ondersteuning van het colocatie-, managed hosting- en managed services-systeem. Deze secundaire ondersteuningssystemen werden niet beschouwd als primaire systemen die binnen het bestek vallen.

Secundaire ondersteuningssystemen	
Productie Applicatie	Beschrijving van de bedrijfsfunctie
Fortinet Firewall	Firewall tussen internet en de Felton Cloud
Cisco (Switching)	Voorziening van netwerkverbinding tussen componenten in Felton Cloud
DELL (HCI en hardware)	Hard en Softwarevoorziening ten aanzien van de Compute, Memory en Storage van Virtuele machines in de Felton Cloud
Microsoft Storagespaces Direct	Voorziening van Storage van Virtuele machines in de Felton Cloud
Microsoft Azure	Alle Microsoft Azure technologie die in onze dienstverlening zit verweven. Vb. Active Directories, Teams en Office.
Microsoft HyperV	Primaire Virtualisatie technologie om onze virtuele machines mee faciliteren.
VMWare	Secundaire Virtualisatie technologie om onze virtuele machines mee faciliteren.
Microsoft SystemCentre Virtual Machine Manager	Managementsoftware voor onze virtuele machines
Zabbix	Monitoring software
Observium	Monitoring software
Rapid7 Insight VM	Vulnerability managementsoftware.

3.3.2 Mensen

De volgende functionele gebieden/ groepen worden gebruikt om de in dit verslag beschreven colocatie, managed hosting en managed services te ondersteunen:

- Felton Cloud team
- Intern beheer team
- Klantteams
- Servicedesk
- Managementteam

3.3.3 Procedures

Servicemanagement:
Het Servicemanagement proces is onderdeel van het Felton Management Systeem (FMS). Het proces beschrijft de manier van continu bijsturen op de kwaliteit van de service aan de klanten van Felton. Als processen duidelijk zijn en geïmplementeerd, kunnen controles worden gedaan om de kwaliteit van onze diensten te bewaken en aan te passen. Het doel van Service Management is ervoor te zorgen dat de geleverde dienstverlening overeenkomst met de afgesproken dienstverlening.

Daarnaast zorgt het ervoor dat de gemaakte afspraken nog overeenkomen met de daadwerkelijke service-behoefte van de klant.

Incident management:
Het incidentmanagementproces behelst de aanmelding, behandeling en afmelding van incident. Als processen duidelijk zijn en geïmplementeerd, kunnen controles worden gedaan om de kwaliteit van onze diensten te bewaken en aan te passen. Incidenten worden geadministreerd in Topdesk.

Het proces begint bij het maken van een incident voor een eindgebruiker. De Servicedeskmedewerker verzamelt alle informatie, zoals contactgegevens, beschrijving van de storing en prioriteit (impact * urgentie). Op basis van de impact en urgentie wordt een prioriteit vastgesteld door de Servicedesk.
Wanneer het incident in behandeling is en het incident managementproces doorloopt dient de melding bewaakt te worden door de Servicedesk en/of incident manager op de voortgang van het incident totdat het incident is opgelost en gesloten in het Topdesk.

Changemanagement:
Changemanagement betreft geplande wijzigingen in de dienstverlening. Afspraken over Changemanagement hebben als doel alle wijzigingen (changes) van de ICT-infrastructuur op gecontroleerde wijze te laten verlopen.

Het doel van het change managementproces binnen Felton is:

- Vastleggen van een gestandaardiseerd proces waardoor changes gecontroleerd worden geïmplementeerd en de risico's worden geminimaliseerd;
- Het adequaat reageren op request for changes (RFC) van de klanten, zodat de service voldoet aan de SLA en de requirements van de klant;
- Zorgdragen dat changes correct worden beoordeeld, geautoriseerd, geïmplementeerd, gedocumenteerd en na implementatie voldoende geëvalueerd worden

Het Changemanagementproces omvat de complete infrastructuur in beheer van Felton. Dat wil zeggen inclusief de ontwikkel-, test-, acceptatie- en productieomgevingen. De primaire componenten in het Change Management proces zijn:

- Hardware: Alle installaties, aanpassingen en verwijderen van hardware
- Software: Installatie, upgrade of verwijderen van software inclusief operating systems
- Back-up schema's of andere reguliere jobs in beheer van Felton
- Werkplek beheer

Het Changemanagementproces bevat vier categorieën, namelijk:

- Spoed change – een change die zo spoedig mogelijk geïmplementeerd moet worden, omdat er een hoge impact of hoge risico's aanwezig zijn voor de klant of Felton. (bv een security patch).
- Standaard change – een change waarbij de impact, risico's en kosten reeds vooraf bekend zijn en een standaardprocedure gehanteerd wordt.
- Non-standaard change – change met weinig impact en risico's waarbij het RFC-template voldoende informatie bevat om deze uit te kunnen voeren.
- CAB- change – Change met een hoge impact en/of risico voor de klant waarbij een Change Implementatie Plan dient te worden opgesteld die wordt beoordeeld door het CAB. Na goedkeuring van het CAB en klant kan de change worden uitgevoerd.

Het CAB staat voor Change advisory board en is verantwoordelijk voor de beoordeling en evaluatie van alle wijzigingen van meer dan geringe omvang. Alle betrokkenen en belanghebbenden zijn hierin vertegenwoordigd, zodat het hele wijzigingstraject beoordeeld kan worden.

Het changemanagementproces wordt volledig geadministreerd in Topdesk. De servicemanagers zijn verantwoordelijk voor alle changes binnen hun klantenteam.

Eventmanagement:
Alle events die voldoen aan specifiek ingestelde triggers worden geregistreerd in Topdesk en doorlopen het incident managementproces.

Er zijn twee software tools die events monitoren en genereren.

- Zabbix: Monitoringstool die 24/7 diverse hardware en netwerkcomponenten monitort.
- Ahsay Back-up: Software die dagelijkse een back-up maakt van (klant)data

Zodra een event wordt getriggerd binnen Zabbix zal, indien het event nog bestaat na (scan-interval + 1) minuten, worden gecontroleerd of er voor dit event in het verleden Topdesk tickets zijn aangemaakt. Hierop kunnen de volgende acties volgen:

- Is er een open ticket? -> Er wordt een update in dit ticket geplaatst.
- Zijn er een of meerdere gesloten tickets? -> De laatste (max 5) tickets worden als verwijzing toegevoegd bij het aanmaken van het ticket.
- Zijn er geen eerdere tickets? -> Er wordt een nieuw ticket aangemaakt.

Indien het ticket juist wordt aangemaakt of geüpdatet, dan zullen de tags in Zabbix worden geplaatst. Lukt het aanmaken of updaten niet, dan wordt dit na (scan-interval + 1) minuten nogmaals geprobeerd totdat dit wel lukt.

Felton gebruikt Ahsay voor het uitvoeren van back-ups. Bij fouten dient een ticket in Topdesk te worden aangemaakt zodat de juist behandelaar(s) deze fouten kunnen herstellen. De controle op fouten en het aanmaken van tickets wordt gescript uitgevoerd. Binnen het script dat is gemaakt wordt op basis van de laatste status(sen) gecontroleerd of actie benodigd is. Hierbij maakt het type dataset uit voor benodigde actie. Is dit het geval, dan wordt een nieuw ticket aangemaakt, of een bestaand ticket voorzien van een update.

Capacitymanagement:
Het capacity management bij Felton is te verdelen in drie hoofdcategorieën. Te noemen Storage, System en Networking. In de categorie Storage vallen SAN, NAS en Interne harde schijven van servers en workstations. In de categorie System vallen alle servers en workstations zowel fysiek als virtueel. In de categorie Networking vallen alle netwerkcomponenten en netwerkconnecties.

Storage
In de categorie Storage wordt a.d.h.v. Zabbix (Felton Monitoring) de capaciteit van SAN's, NAS en Interne schijven van servers op het gebied van schijfruimte en Read/Write performance gemeten. De minimale schijfruimte is per device gedefinieerd en varieert van minimaal 0% schijfruimte tot 90% schijfruimte.

System
In de categorie System wordt a.d.h.v. Zabbix de capaciteit van servers op het gebied van CPU en werkgeheugen gemeten. Voor alle devices zijn de thresholds standaard ingesteld op:

- Memory: >90% commited bytes voor een periode van vijf minuten

- Memory: >70% pagefile usage voor een periode van vijf minuten
- CPU: >95% Processor time voor een periode van vijf minuten.

Networking

In de categorie Networking wordt de capaciteit bijgehouden door Observium. Op het gebied van belasting en bandbreedte zijn de thresholds standaard ingesteld op >95% Recieve/Send utilization voor een periode van 5 minuten. Bij overschrijden van deze thresholds wordt automatisch een e-mail en/of bericht verstuurd.

Configurationmanagement:

Het primaire doel van het Asset & configuration managementproces is ervoor te zorgen dat alle configuration items die in beheer zijn bij Felton geregistreerd staan in de CMDB met de juiste gegevens. Het CMDB wordt in Topdesk geadministreerd zodat het configurationmanagement proces naadloos aansluit op alle andere processen die worden gedocumenteerd binnen Topdesk.

Klachtenprocedure:

Om de kwaliteit van dienstverlening te bewaken en als ondersteuning van de continuous improvement dienen klachten die binnenkomen op een goede en uniforme manier te worden afgehandeld. De klachtenprocedure heeft als doelstelling dat:

- Klachten niet verloren gaan in de dagelijkse praktijk
- Klachten een eigenaar krijgen
- Met de juiste prioriteit naar klachten wordt gekeken
- Als het onderwerp van een klacht een structureel karakter heeft, de processen bij Felton kunnen worden aangepast (Continuous improvement).
- Er een doeltreffend klachten behandelplan wordt opgesteld en uitgevoerd
- Klantentevredenheid voldoende is en voldoende blijft.

Cloudmanagment:

De Felton Cloud is een Private Cloud waar klanten van Felton Virtuele Machines (VM) afnemen. Om de VMs van klanten beschikbaar, veilig en integer te houden zijn een aantal processen gedefinieerd.

1. Aanmaken van resources
2. Aanpassen van resources
3. Updaten van resources
4. Verwijderen van resources
5. Capaciteit Resource gebruik rapportage Felton Cloud
6. Beschikbaarheid. Event gedreven monitoring en ticketing.

Al deze processen vallen onder het Felton Cloud Management en zijn in detail in het FMS gedocumenteerd als onderdeel van de bedrijfsvoering.

Procedure Back-up:

Felton maakt periodiek een back-up. Deze back-up omvat zowel de eigen data van Felton, als de data van haar klanten.

Door het maken van deze back-up verzekert Felton zich ervan dat het eigen data, of data van haar klanten kan herstellen in geval van verstoringen en calamiteiten. Hierbij kan gedacht worden aan het

onbedoeld verwijderen/overschrijven van bestanden, virusinfecties of hardware falen.
Met elke klant is contractueel afgesproken welke back-up strategie wordt aangehouden. Deze contracten bevatten in ieder geval de volgende informatie:

- Retentie
- Selectie (aantal servers)
- Back-up schema
- Eventuele archivering (jaarback-ups)

Locaties:
De back-up infrastructuur van Felton is verdeeld over twee locaties. Dit zijn het datacenter in Groenekan en Alblasserdam. De primaire back-up server bevindt op Datacenter Groenekan. De back-ups van File, Mail en SQL-servers worden via een beveiligde internetverbinding naar back-up-server in Groenekan weggeschreven. Deze server repliceert betreffende informatie naar een Replicatie server in het datacenter in Alblasserdam. Hierdoor is er voor File, Mail en SQL altijd een externe back-up (verdeeld over twee locaties) welke in geval van een calamiteit teruggezet kan worden.

Restore
Restores (het terugzetten van een back-up) kunnen via het ticketsysteem worden aangevraagd door iedere gebruiker. Als de te restoren data niet om persoonlijke gebruikersdata gaat, maar om bijvoorbeeld serverdata, dient er een goedkeuring gegeven te worden door een manager. De restore wordt altijd uitgevoerd op een tijdelijke locatie waar de aanvrager de gerestorde data kan controleren. Als de restore is goedgekeurd door de aanvragen wordt de data verplaatst naar de definitieve plaats.

Disaster Recovery
Ondanks dat de apparatuur van Felton zich in een beveiligd/gecertificeerd datacenter bevindt, bestaat er een kans dat de apparatuur door een calamiteit onbruikbaar wordt. Daarom zijn de back-ups van Felton zo ingericht dat er een recovery gedaan kan worden o.b.v. de back-ups. De back-up wordt dagelijks uitgevoerd en gecontroleerd op juist verloop. Een recovery kan worden gedaan met een maximaal dataverlies van 24 uur.

Encryptie
De back-ups die worden gemaakt worden versleuteld. De toegepaste techniek hiervoor is gedocumenteerd in het overzicht “Crytografische maatregelen”.

De encryptiesleutels voor de back-up worden gedocumenteerd in Password State.
Van de encryptiesleutel van de back-up van Password State is een hardcopy in de kluis aanwezig. Met deze mitigerende maatregel borgen we dat tijdens een verstoring van Passwordstate we altijd een back-up kunnen terugzetten van alle encryptiesleutels van de back-up omgeving.

RPO/ RTO
De RPO van de back-ups is maximaal 24 uur.
De RTO voor een file of directory recovery is 1 uur.
De RTO voor een disaster recovery is maximaal 2 weken. Doordat er volledig decentraal gewerkt kan worden heeft dit geen impact op het primaire proces. De RPO en RTO van klanten is vastgelegd in de contracten die we met de specifieke klanten hebben

Procedure HR:
Het HR-proces beschrijft de manier van in dienst, doorgroei en uit dienst van medewerkers. Als processen duidelijk zijn en geïmplementeerd, voldoet Felton aan de wet- en regelgeving en zijn alle benodigde actie uitgevoerd om mensen in- en uit dienst te laten treden. Binnen HR zijn er verschillende onderwerpen die beheerd worden. Dit start bij het werven, selecteren en onboarden van nieuwe medewerkers en eindigt bij het afscheid en de financiële afrekening van medewerkers. De proceseigenaar van de HR-processen is de HR-manager. De proceseigenaar heeft zicht op het gehele proces en legt daarmee de procedure vast. De proceseigenaar bepaalt de doelstellingen en stuurt het proces mede op basis van KPI's en SLA's. De proceseigenaar is verantwoordelijk voor alle activiteiten binnen het proces en voert op regelmatige tijdstippen audits uit om de efficiëntie van het proces te toetsen en waar nodig bij te sturen.

Procedure meldplicht datalekken:
Het doel van de procedure meldplicht datalekken is ervoor zorgdragen dat medewerkers van Felton in geval van een datalek deze procedure volgt om de impact op de organisatie te minimaliseren.

Wat is een datalek
Bij een datalek gaat het om toegang tot persoonsgegevens of vernietiging, wijziging of vrijkomen van gegevens zonder dat dat de bedoeling is van de organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook het onrechtmatig verwerken van gegevens. Er is sprake van een datalek als er inbreuk is op de beveiliging. Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Melden van een datalek
Een datalek wordt gemeld middels het formulier meldloket datalekken op website van de Autoriteit Persoonsgegevens.

Klant/leveranciersovereenkomst
Indien werkzaamheden worden uitbesteed aan derden dan is de verwerkersregeling van de AVG van toepassing. De volgende zaken worden in de overeenkomst met de leverancier/ klant overeengekomen en vastgelegd.

Verwerker buiten Nederland
De vestigingsplaats van de verwerker is voor de meldplicht datalekken niet relevant. Ook datalekken die plaatsvinden bij een buitenlandse verwerker (die gevestigd is in een andere EU-lidstaat of in een land buiten de EU) moeten worden gemeld aan de Autoriteit Persoonsgegevens.

3.3.4 Informatie

Om haar dienstverlening uit te kunnen voeren gebruikt Felton informatie. Op alle informatiesoorten is een impact- en risicoanalyse uitgevoerd. Hoe Felton gegevens behandeld, wordt bepaald door de risicoscore.

Felton heeft de volgende informatie geïdentificeerd en beoordeeld:

- Financiële informatie
- Personeelsinformatie
- Back-up (eigen informatie)

- Back-up (klant informatie)
- Klantdocumentatie
- Wachtwoorden
- Tickets en persoonsinformatie klanten

Naast eigen informatie komt Felton, door de aard van haar dienstverlening, in aanraking met gegevens van haar klanten. Felton behandelt deze gegevens conform de contracten met haar klanten, verwerkersovereenkomsten en geldende wet- en regelgeving.

3.4 Relevante aspecten van interne controle

3.4.1 Controleomgeving

De controleomgeving bij Felton vormt de basis voor de andere gebieden van de interne controle. Zij zet de toon van de organisatie en beïnvloedt het controlebewustzijn van het personeel. Tot de componenten van de controleomgeving behoren de rol van het Management Team, de organisatiestructuur en de taken en verantwoordelijkheden.

3.4.2 De rol van het management team

Informatie is binnen de dienstverlening van Felton de belangrijkste grondstof. Klanten, medewerkers, leveranciers, aandeelhouders en andere belanghebbenden van Felton moeten er op kunnen vertrouwen dat hun informatie én Persoonlijk Identificeerbare Informatie (PII) bij Felton in veilige handen is. Daarnaast is de borging van de kwaliteit van dienstverlening belangrijk voor Felton en haar klanten.

Het management van Felton is zich ervan bewust dat zij een grote invloed heeft op de organisatie. Door actief deel te nemen aan de beheersing van het managementsysteem, zet zij de toon voor de organisatie.

Het managementteam heeft de volgende rol ten aanzien van de controleomgeving:

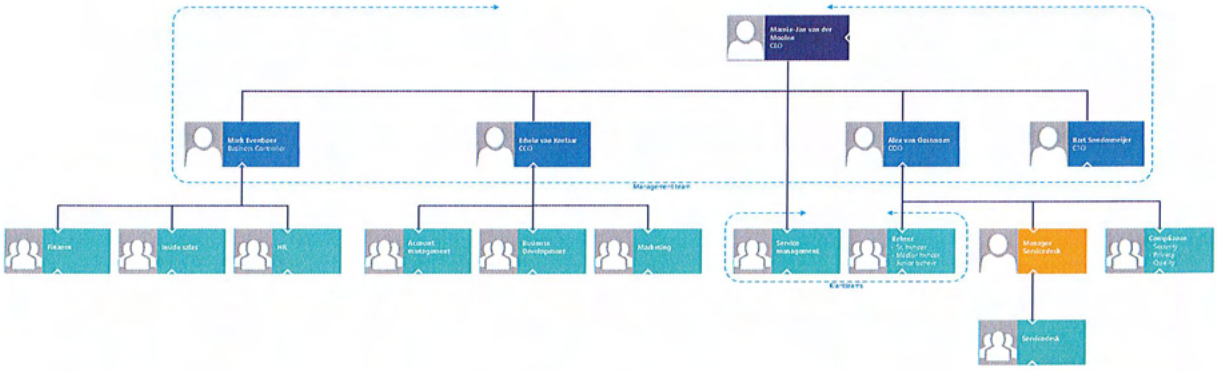
- De eindverantwoordelijkheid voor de prestaties ligt bij het Management Team van Felton;
- Het Management Team van Felton komt wekelijks samen. Onderdeel van deze meeting is de voortgang op verbeterprojecten, prestatie-resultaten en operationele issues;
- Het Management Team stuurt bij waar nodig;
- Het Management Team is onderdeel van interne en externe audits.

3.4.3 Organisatiestructuur

De volgende afdelingen en/of teams hebben een rol in het beheer, of gebruik van de controleomgeving:

- Het managementteam is verantwoordelijk voor de algemene prestaties van Felton. Dit omvat ook de verantwoordelijkheid voor het SOC-controlekader en gerelateerde processen.
- HR is verantwoordelijk voor de HR-processen en -procedures.
- Het Compliance Team is verantwoordelijk voor het opstellen, onderhouden en continu verbeteren van het Felton Management System (FMS), waarbij invulling wordt gegeven aan de beveiliging, kwaliteit en privacy-management van onze dienstverlening.

- Service Management is verantwoordelijk voor het ontwerp en de contractuele afspraken van diensten
- De klantteams zijn verantwoordelijk voor de uitvoering van de contractuele afspraken van diensten



3.4.4 Beheersmaatregelen

Om informatiebeveiliging, kwaliteit en privacy te borgen, heeft Felton het Felton Management System (FMS) opgezet en geïmplementeerd dat voldoet aan de volgende normen:

- **NEN-ISO/IEC 27001/27002** *Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging*
- **NEN-EN-ISO 9001** *Kwaliteitsmanagementsystemen*
- **NEN-ISO/IEC 27701** *Veiligheidstechnieken - Uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor privacy-informatiemanagement*
- **NEN 7510-1** *Informatietechnologie – Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging*

Het FMS wordt onderhouden en daar waar van mogelijk continu verbeterd. Bij het opstellen van het FMS is rekening gehouden met schaalbaarheid en eenvoudige toepasbaarheid bij toekomstige groei.

3.4.5 Controleactiviteiten

Integratie met risicobeoordeling

Naast de beoordeling van de risico's heeft het management de nodige acties vastgesteld en uitgevoerd om die risico's aan te pakken. Om de risico's aan te pakken, zijn controleactiviteiten in werking gesteld om ervoor te zorgen dat de acties correct en efficiënt worden uitgevoerd. Controleactiviteiten dienen als mechanismen voor het beheer van de verwezenlijking van de beveiligings- en beschikbaarheidsbeginselen.

3.4.6 Interne communicatie interne beheersing

Het management heeft alle documentatie van het kwaliteitssysteem gedocumenteerd in het Felton Management Systeem (het FMS). De documentatie is voor alle medewerkers toegankelijk zodat men daar processen, procedures, bewijsstukken uit audits, schema's, overzichten kunnen vinden naast alle andere zaken die belangrijk zijn voor ons managementsysteem.

Samenvatting Informatiebeveiligingsbeleid, privacy en kwaliteit
Alle nieuwe medewerkers krijgen tijdens het introductieprogramma een samenvatting aangeboden waarin de belangrijkste zaken uit ons managementsysteem zijn samengevat. Hierin wordt ook verwezen naar het FMS ter naslag.

Introductie Informatiebeveiligingsbeleid, privacy en kwaliteit
Alle nieuwe medewerkers krijgen tijdens het introductieprogramma een presentatie waarin een afvaardiging van het Security, Privacy en Quality Forum de nieuwe medewerkers meeneemt in het kwaliteitssysteem van Felton. Er wordt een presentielijst bijgehouden van alle deelnemers. Op deze manier weten nieuwe medewerkers wat er van ze wordt verwacht t.a.v. managementsysteem. De focus ligt hierbij op continuous improvement.

Terugkerende informatiesessies/onderwerpen
Tijdens diverse terugkerende informatiesessie informeren wij al ons personeel van wijzigingen, addities en andere belangrijke updates omtrent ons managementsysteem. Dit kunnen diverse onderwerpen zijn, bijvoorbeeld het aanpassen van bepaalde processen aan de hand van een verbetervoorstel, maar ook het implementeren van een nieuwe securityoplossing.

3.4.7 Toezicht en controles

Controleactiviteiten

Het management en de organisatie van Felton worden periodiek gecontroleerd. Hierbij wordt gekeken naar de werking en effectiviteit van het Felton Management Systeem en worden eventueel aanbevelingen gedaan voor verbetering. Deze controles zijn gebaseerd op de ISO27001, ISO9001, ISO27701 en NEN7510 normen.

Felton heeft de volgende controleactiviteiten geïmplementeerd

- Interne audits
- Externe audits
- Risicobeoordeling
- Periodieke specifieke controles zoals: review beleid, controle autorisaties, controle fysieke toegang, controle technische implementatie, beoordeling van leveranciers en Pen-testen
- Beoordeling KPI-prestaties

Het Compliance Team van Felton komt maandelijks bijeen om de resultaten van de controleactiviteiten te bespreken en waar nodig te evalueren.

3.4.8 Evalueren en communiceren van tekortkomingen

Een organisatie is continu in beweging. Hierdoor kan het voorkomen dat bij het uitvoeren van controle-activiteiten blijkt dat er tekortkomingen of verbeterkansen zijn. Daarnaast kunnen tekortkomingen worden gemeld door belanghebbenden door middel van het klachtenproces.

Bij tekortkomingen met een hoge impact wordt het managementteam direct geïnformeerd. Daarnaast rapporteert het compliance team periodiek een samenvatting van de tekortkomingen uit de audits, risicobeoordeling, klachtenprocedure en andere controles. Bij deze rapportage worden ook de positieve resultaten en opgemerkte kansen uit de controles gerapporteerd.

3.5 Sub-serviceorganisaties

Felton past de carve-out methode toe met betrekking tot haar sub serviceorganisaties.

Felton beheert sub-serviceorganisaties op basis van best practices volgens ISO 27002. Wanneer mogelijk controleert Felton de SOC2 type2, of soortgelijke verklaring van haar sub-serviceorganisaties.

Voor haar dienstverlening maakt Felton gebruik van de volgende sub-serviceorganisaties:

Sub-serviceorganisatie	
Naam	Dienst
Dataplace	Housing en fysieke beveiliging van de Felton Cloud
Eurofiber	Connectiviteit Felton Cloud
Microsoft	Levering public cloud diensten
Topdesk	Levering Service Management Systeem (SaaS)

De sub service organisaties hebben de volgende controls geïmplementeerd

- Business Continuity management
- Change management
- Data security
- Fysieke beveiliging
- Identity and access management
- Security incident management
- Vulnerability management

3.6 Risicobeoordelingsproces

Het doel van het risicoanalyseproces is te beoordelen hoe groot een risico's is en daarmee de aandacht van het management te richten op de belangrijkste bedreigingen, kansen en om de basis te leggen voor de risicobehandeling.

Risicobeoordeling heeft alles te maken met het meten en prioriteren van risico's, zodat risiconiveaus worden beheerd binnen gedefinieerde tolerantiedrempels (risicobereidheid). Hiermee wordt voorkomen dat te zware maatregelen worden getroffen en/of mogelijke kansen worden gemist. Een risico waarvan de kans dat het optreed klein is en waarvan de impact eveneens laag is, zal niet in aanmerking komen voor een risicobeperkende maatregel. De kosten daarvan wegen vermoedelijk niet op tegen de schade die men voorkomt. Andersom zal het wel rendabel zijn een risico met een hoge kans van optreden en een hoge impact te mitigeren.

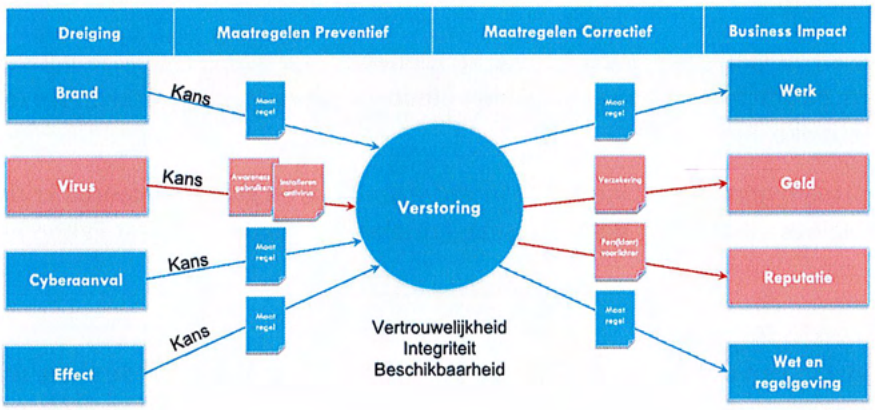
Binnen Felton voeren we de stappen in het risicoanalyseproces en risicobehandelingsproces jaarlijks uit. Daarnaast kunnen zich gebeurtenissen voordoen die leiden tot een nieuwe risicobeoordeling en mogelijke gevolgen voor de risicobehandeling. Voorbeelden van gebeurtenissen die Felton ziet als basis om het risicobeoordelingsproces uit te voeren zijn onder andere de initiële vaststelling van de start van een nieuw project, aanschaf of uitfasering van hard- of software, wijzigingen in wet- en regelgeving (zoals bijv. de AVG in 2018), een fusie, overname of afstoting, of een grote herstructurering. Sommige risico's zijn dynamisch en vereisen continue monitoring en beoordeling, zoals bepaalde markt- en productierisico's. Andere risico's zijn meer statisch en vereisen periodieke herbeoordeling.

Het beoordelen van risico's bestaat uit het toewijzen van waarden aan elk risico én aan elke opportunity op basis van gedefinieerde criteria.

Felton voert het risicobeoordelingsproces en het risicobehandelingsproces uit volgens de vlinderdas of bow-tie methode. De vlinderdas methode is een kwalitatieve risicoanalyse methode, waarmee op een systematische wijze een beeld kan worden verkregen van de risico's die in een organisatie aanwezig zijn en van de preventieve en correctieve beheersmaatregelen die hierop (kunnen) worden ingezet. Risico's, bedreigingen, preventieve en correctieve beheersmaatregelen zijn in één model verenigd. Centraal staat de verstoring, met links de oorzaken en rechts de gevolgen. Beheersmaatregelen toont men in de vorm van barrières.

De vlinderdas (bow-tie) methode is een eenvoudige manier in de vorm van een figuur die de paden analyseert en beschrijft van een verstoring vanaf de mogelijke oorzaken tot en met de ongewenste gevolgen. Essentie van de vlinderdas ligt in het aanbrengen van beheersmaatregelen, preventief of correctief, tussen de oorzaken en de verstoring, en tussen de gebeurtenis en de gevolgen. Een vlinderdas kan opgebouwd worden vanuit interviews met medewerkers uit verschillende lagen van de organisatie.

Het resultaat is een eenvoudig diagram dat de vele mogelijke paden toont en de maatregelen die genomen moeten worden (zie onderstaande figuur en bijlage 1 voor voorbeelden).

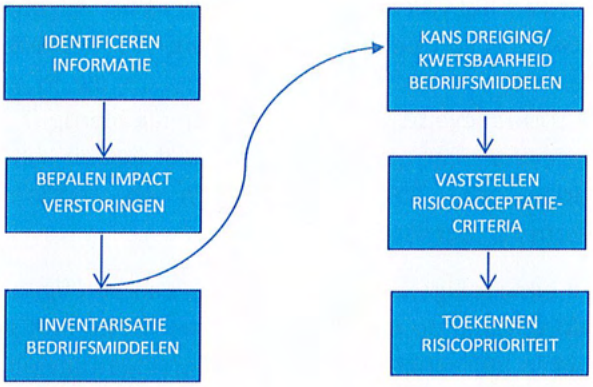


Het risicobeoordelingsproces bestaat uit 6 stappen:

1. Identificeren van voor de organisatie kritieke informatie (waarbij ervan uitgegaan wordt dat de verstoring reeds heeft plaatsgevonden);
2. Bepalen van de impact (financieel, reputatie etc.) van de verstoringen (Business Impact Analyse);
3. Inventarisatie van bedrijfsmiddelen en de bedreigingen die zich kunnen voordoen met betrekking tot deze bedrijfsmiddelen;
4. Bepalen van de kans dat een dreiging zich voordoet en van de kwetsbaarheid van de betrokken bedrijfsmiddelen;
5. Vaststellen risicoacceptatiecriteria;
6. Toekennen risicoprioriteit op basis van de formule (impact x kans x kwetsbaarheid).

Felton heeft 3 deelcriteria gedefinieerd, deze komen in stap 2 en 4 aan bod.

De onderstaande figuur geeft een overzicht van de verschillende stappen binnen het Risicobeoordelingsproces.



Identificeren kritieke informatie:
Het risicobeoordelingsproces begint met het identificeren van kritieke informatie, op basis van ongewenste gebeurtenissen/verstoringen die betrekking hebben op de beschikbaarheid, integriteit en/of vertrouwelijkheid van deze informatie. Bijv. de persoonsgegevens van cliënten (kritieke informatie) liggen op straat, omdat de server is gehackt (ongewenste gebeurtenis welke betrekking heeft op vertrouwelijkheid).

innen Felton hebben wij dit stadium breed uitgewerkt. Medewerkers van verschillende functies en niveaus zijn bij dit proces betrokken geweest. Aan het einde van deze stap beschikken we over een uitgebreide lijst van kritieke informatie.

Met het managementteam nemen we jaarlijks de in voorgaande jaren geïdentificeerde kritieke informatie door. Wijzigingen in de voor de organisatie kritieke informatie verwerkt Felton hier ook tussentijds in.

Bepalen impact verstoringen:

De impact (of gevolg) van een ongewenste gebeurtenis/verstoring verwijst naar de mate waarin zo'n verstoring Felton als geheel, bedrijfseenheden, bedrijfsfuncties of projecten met grote impact zou kunnen beïnvloeden. Verstoringen kunnen impact hebben op verschillende gebieden.

Voor het bepalen van de impact van een verstoring hanteert Felton de volgende categorieën van impact:

- Verstoring van werkzaamheden (Business Impact);
- Operationeel verlies;
- Reputatieschade;
- Falen in voldoen aan regelgeving/ wetgeving en/of compliance voorwaarden;
- Clientletsel of -schade.

Een verstoring kan impact hebben op meerdere categorieën. Wanneer een impactbeoordeling wordt toegewezen aan een verstoring, wijst Felton de rating toe voor de hoogste verwachte gevolgen. Wanneer bijvoorbeeld een verstoring impact zal hebben op de reputatie van Felton en op een onderbreking van werkzaamheden, waarbij aan reputatieschade een impactclassificatie wordt

toegekend van 4 en aan onderbreking van werkzaamheden een impactclassificatie van 3, dan is voor deze verstoring de impactclassificatie 4.

Samenvattend, de categorie met de hoogste impactclassificatie wordt gebruikt bij het vaststellen van de risicoacceptatie, zoals uitgewerkt in paragraaf 2.6 van dit document.

Inventarisatie bedrijfsmiddelen en bedreigingen:
Voor alle verstoringen met een Business Impact van 3 of 4 stelt Felton vast wat de daarbij behorende bedrijfsmiddelen (assets) zijn. De verstoringen en daarmee ook de kritieke informatie is te relateren aan meerdere bedrijfsmiddelen van verschillende typen. Hierin is een gelaagdheid zichtbaar. Hieronder geven wij een voorbeeld ter illustratie. Na het identificeren van de bedrijfsmiddelen en de (be)dreigingen heeft Felton bepaald wie de 'eigenaar' is van een bedrijfsmiddel, de 'asset owner'. Asset owners binnen Felton zijn die medewerkers die het meest betrokken zijn bij de bedrijfsmiddelen. Bijvoorbeeld de Security Officer, de systeembeheerder en de applicatiebeheerder.

Bepaling kans van de dreiging en kwetsbaarheid van bedrijfsmiddelen
De asset owners van Felton hebben ten minste eens per jaar overleg om de kans dat de geïdentificeerde dreiging zich voordoen en om de kwetsbaarheid van het optreden van bedreigingen voor deze bedrijfsmiddelen te (her)beoordelen.

Per dreiging heeft Felton de kans of waarschijnlijkheid (likelihood) dat een dergelijke dreiging zich voor zal doen bepaald.

Voor dreigingen uit het verleden, heeft Felton gekeken naar het aantal keren per periode dat een dreiging zich voor heeft gedaan en heeft daar waar mogelijk gebruik gemaakt van statistische cijfers. Ook gebruikt Felton data en benchmarks van externe partijen voor veel voorkomende dreigingen, waaronder bijvoorbeeld informatie over datalekken van de Autoriteit Persoonsgegevens. De geschatte frequentie koppelt Felton aan de kwalitatieve termen (vaak, mogelijk, zeldzaam).

Voor dreigingen waarbij het niet goed mogelijk is om tot een geschatte frequentie te komen, drukt Felton de waarschijnlijkheid ook uit op basis van de kwalitatieve termen (vaak, mogelijk, zeldzaam).

Felton beoordeelt eveneens jaarlijks de kwetsbaarheid van de bedrijfsmiddelen voor de dreigingen. Op basis van onderstaande schaalindeling geven de asset owners aan hoe hoog zij de kwetsbaarheid van de bedrijfsmiddelen inschatten. Hieruit volgt de beoordelingsscore voor de kwetsbaarheid.

Vaststellen risicobereidheid:
De IS&QF-leden besluiten welke kwantitatieve score het meest overeenkomt met de risicobereidheid van de organisatie. Hierbij baseren de IS&QF-leden zich op de resultaten uit de vorige stappen.

Felton kiest ervoor om risico's met een waarde lager dan 18 te accepteren. Risico's met een waarde van 18 of hoger behoeven maatregelen.

Toekennen risicoprioriteit:

Risico-prioritering is het proces van het bepalen van prioriteiten voor risicobeheer door het risiconiveau te vergelijken met de in de vorige stap bepaalde risiconiveaus en tolerantiedrempels. Zoals bij het vaststellen van de risicoacceptatiecriteria benoemt kijkt Felton niet alleen in termen van financiële impact en waarschijnlijkheid, maar ook naar subjectieve criteria zoals reputatieschade of financiële schade.

Uitkomst van het toekennen van de risicoprioriteit (inclusief de risico's waarop geen actie zal worden ondernomen) is een overzicht met de voor Felton belangrijkste risico's inclusief de daarbij behorende bedrijfsmiddelen. Dit overzicht vormt de basis voor het risicobehandelingsproces en het risicobehandelingsplan. In de bespreking van de risico-prioritering kent Felton ook risico-eigenaren toe. In de praktijk zijn dit vaak dezelfde personen als de asset owners.

3.7 Relevante wijzigingen in het systeem

De periode Q1 2023 betreft een initiële verslagperiode. Eventuele wijzigingen op het systeem bij toekomstige periodes, zullen hieronder worden toegelicht.

3.8 Toepasselijke criteria en controles voor vertrouwensdiensten die zijn ontworpen om de serviceverplichtingen en systeemvereisten van Felton B.V. te bereiken

Common criteria; Security

ID	Categorieën van Common Criteria	Common Criteria TSP referentie	Control Activity nummer
1	Control Environment	CC1.1	1, 2, 3, 4, 5
2		CC1.2	1, 2, 4
3		CC1.3	1, 2, 3, 4, 5
4		CC1.4	1, 2, 3, 4, 5, 6, 7
5		CC1.5	1, 2, 3, 4, 5,
6	Communication and Information	CC2.1	1
7		CC2.2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
8		CC2.3	1, 2, 3, 4, 5, 6, 10, 11,

9	Risk Assessment	CC3.1	1, 2, 4, 8, 11, 14, 15, 16
10		CC3.2	1, 2, 3, 4, 5, 6, 7, 8
11		CC3.3	1
12		CC3.4	1, 2, 3, 4, 5
13	Monitoring Activities	CC4.1	1, 2, 3, 4, 5, 6, 7, 8
14		CC4.2	1, 2, 3
15	Control Activities	CC5.1	1, 2, 3, 4, 5, 6
16		CC5.2	2, 3, 4
17		CC5.3	1, 2, 3, 4, 5, 6
18	Logical and Physical Access Controls	CC6.1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
19		CC6.2	1, 2, 3
20		CC6.3	1, 2, 3
21		CC6.4	1, 2, 3
22		CC6.5	1, 2
23		CC6.6	1, 2, 3, 4
24		CC6.7	1, 2, 3, 4
25		CC6.8	1, 2, 3, 4, 5
26	System Operations	CC7.1	1, 2, 3, 4, 5
27		CC7.2	1, 2, 3, 4
28		CC7.3	1, 2, 3
29		CC7.4	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
30		CC7.5	1, 2, 3, 4, 5, 6
31	Change Management	CC8.1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
32	Risk Mitigation	CC9.1	1, 2
33		CC9.2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

Additionele criteria; AVAILABILITY

ID	Additionele Criteria Availability TSP referentie	Control Activity nummer
34	A1.1	1, 2, 3
35	A1.2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
36	A1.3	1, 2

Additionele criteria;

Vertrouwelijkheid

ID	Additionele Criteria Vertrouwelijkheid TSP referentie	Control Activity nummer
37	C1.1	1, 2
38	C1.2	1, 2

3.9 Beheersmaatregelen voor gebruikersorganisaties

Bij het ontwerpen van haar systeem heeft Felton B.V. overwogen dat bepaalde aanvullende controles door gebruikersorganisaties zullen worden geïmplementeerd om bepaalde controledoelstellingen te bereiken die in dit rapport onder hun controle of toezicht zijn opgenomen:

- Klanten zijn verantwoordelijk voor het opzetten van fysieke beveiligingen voor alle werkstations, servers en communicatie hardware die communiceren met hun beheerde hostingomgeving en die zijn ondergebracht in hun faciliteiten of andere locaties.
- Klanten zijn verantwoordelijk voor het melden van eventuele verwerkingsproblemen aan Felton B.V. en voor het verlenen van de hulp die nodig is om problemen op te lossen.
- Na kennisgeving van een onderhoudsvenster moet de klant tijdig passende actie ondernemen op basis van de verzonden meldingen.
- De klant is verantwoordelijk voor de controle op de toegang tot functionaliteit en gegevens die door zijn toepassing worden gebruikt. Dit omvat het gebruik van toepassings-configuratieparameters en databaseconfiguratie.
- De klant is verantwoordelijk voor het identificeren van upgrades/wijzigingen/patches die moeten worden aangebracht op de werkstations/netwerken/omgeving van de gebruiker.
- De klant is verantwoordelijk voor het opgeven van de initiële firewallinstellingen en voor het initiëren van eventuele wijzigingen in de bestaande configuraties indien nodig.
- De klant is verantwoordelijk voor het beheer van de logische toegang tot de Managed Services en daarbij behorende portal accounts.
- De klant is verantwoordelijk voor het beheer van lokale gebruikers- en beheerdersaccounts op zijn servers.
- De klant is verantwoordelijk voor het adequaat monitoren en helpen bij het oplossen van change management tickets, indien nodig.
- De klant is verantwoordelijk voor het verkrijgen, bewaken en op de juiste manier gebruiken van SSL-coderingsclientinstellingen.
- De klant is verantwoordelijk voor het aanvragen van de start van het gegevensherstelproces, indien nodig.

3.10 Controls van de trust services criteria die niet relevant zijn voor het systeem

Binnen de gekozen categorieën (Beveiliging, Beschikbaarheid en Vertrouwelijkheid) waren er geen criteria voor de trusted services die als niet relevant voor het systeem werden beschouwd.

De categorie Privacy werd uitgesloten omdat de SOC II Privacy criteria niet leidend zijn binnen de Europese Economische Ruimte.

De (twee) aanvullende criteria met betrekking tot integriteit werden uitgesloten omdat alle toepasselijke risico's werden gedekt door de integriteitscriteria van de gemeenschappelijke criteria (Common Criteria).